CLAIMS

1. An encryption method for obtaining ciphertext from plaintext, comprising the steps of:

creating a composite vector by adding a random number vector whose components are a plurality of arbitrarily selected random numbers to a plaintext vector having a plurality of components obtained by dividing a plaintext to be encrypted; and

obtaining a ciphertext by using the created composite vector and a publicized public vector.

2. The encryption method of claim 1, wherein

a result of product-sum operation of the components of said composite vector and the components of said public vector is made the ciphertext.

3. The encryption method of claim 1, wherein

a remainder formed by dividing a result of product-sum operation of the components of said composite vector and the components of said public vector by a modulus is made the ciphertext.

4. An encryption method for obtaining ciphertext from plaintext, comprising the steps of:

creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random

numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts; and

obtaining a ciphertext by using the created third vector and a fourth vector whose (k+n) components $D_i (1 \leqq i \leqq k+n)$ are respectively set such that $D_i = d/d_i$ (where $d = d_1 d_2 \ldots d_{k+n}$) by using an integer d_i.

5. The encryption method of claim 4, wherein

the ciphertext is obtained based on a product-sum operation of the components of said third vector and components of a public-key vector modulo-transformed based on said fourth vector.

6. An encryption method for obtaining ciphertext from plaintext, comprising the steps of:

creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts; and

obtaining a ciphertext by using the created third vector and a fourth vector whose (k+n) components V_i $(1 \leqq i \leqq k+n)$ are respectively set such that $V_i = (d/d_i) \cdot v_i$ (where $d = d_1 d_2 \ldots d_{k+n}$) by using an integer d_i.

7. The encryption method of claim 6, wherein

$\gcd(V_i, d_i) = 1$ is satisfied.

8. The encryption method of claim 6, wherein

the ciphertext is obtained based on a product-sum operation of the components of said third vector and components of a public-key vector modulo-transformed based on said fourth vector.

9. An encryption method for obtaining ciphertext from plaintext, comprising the steps of:

creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts; and

obtaining a ciphertext by using the created third vector and L sets ($L \geqq 2$)of fourth vector whose (k+n) components $D_i^{(y)}$ ($1 \leqq i \leqq k+n$, $1 \leqq y \leqq L$)are respectively set such that $D_i^{(y)} = d^{(y)}/d_i^{(y)}$ (where $d^{(y)} = d_1^{(y)} d_2^{(y)} \ldots d_{k+n}^{(y)}$) in each set by using L sets of integers $d_i^{(y)}$.

10. The encryption method of claim 9, wherein

the ciphertext is obtained based on a product-sum operation of the components of said third vector and components of a public-key vector modulo-transformed based on said fourth vector.

11. An encryption method for obtaining ciphertext from plaintext, comprising the steps of:

creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts; and

obtaining a ciphertext by using the created third vector and L sets($L \geqq 2$)of fourth vector whose (k+n) components $V_i^{(y)}$ ($1 \leqq i \leqq k+n$, $1 \leqq y \leqq L$)are respectively set such that $V_i^{(y)} = (d^{(y)}/d_i^{(y)}) \cdot v_i^{(y)}$ (where $d^{(y)} = d_1^{(y)} d_2^{(y)} \ldots d_{k+n}^{(y)}$) in each set by using L sets of integers $d_i^{(y)}$ and random numbers $v_i^{(y)}$.

12. The encryption method of claim 11, wherein $\gcd(V_i^{(y)}, d_i^{(y)}) = 1$ is satisfied.

13. The encryption method of claim 11, wherein $\gcd(d_i^{(y)}, d_j^{(y)}) = 1$ ($1 \leqq j \leqq k+n$) is satisfied.

14. The encryption method of claim 11, wherein

the ciphertext is obtained based on a product-sum operation of the components of said third vector and components of a public-key vector modulo-transformed based on said fourth vector.

15. An encryption method for obtaining ciphertext from plaintext, comprising the steps of:

creating a fourth vector having K (= k+n+h) components by adding together a first vector having k components obtained by

dividing a plaintext to be encrypted, a second vector whose components are n arbitrarily selected random numbers and a third vector having h components indicating information identifying positions of said k components or said n components; and

obtaining a ciphertext by using the created fourth vector and a publicized fifth vector.

16. The encryption method of claim 15, wherein

the ciphertext is composed of a plurality of blocks obtained by using said fourth vector and said fifth vector, and positions of said h components in said fourth vector are identical in each block.

17. The encryption method of claim 15, wherein

the ciphertext is composed of a plurality of blocks obtained by using said fourth vector and said fifth vector, and positions of said k components or said n components in said fourth vector in each block are decided according to said k components in the previous block.

18. The encryption method of claim 15, wherein

the ciphertext is composed of one block obtained by using said fourth vector and said fifth vector and a plurality of blocks obtained by using said fifth vector and said fourth vector in which h components of said third vector are substituted with h components obtained by dividing a plaintext, and positions of (k+h) components

or said n components in said fourth vector in each block are decided according to said k or (k+h) components obtained by dividing the plaintext in the previous block.

19. The encryption method of claim 15, wherein

said fifth vector is generated using a sixth vector whose components D_i ($1 \leqq i \leqq K$)are respectively set such that $D_i = (d/d_i)$ (where $d = d_1d_2...d_K$) by using an integer d_i.

20. The encryption method of claim 19, wherein

the ciphertext is obtained based on a product-sum operation of the components of said fourth vector and components of said fifth vector modulo-transformed based on said sixth vector.

21. The encryption method of claim 15, wherein

said fifth vector is generated using a sixth vector whose components V_i ($1 \leqq i \leqq K$)are respectively set such that $V_i = (d/d_i) \cdot v_i$ (where $d = d_1d_2...d_K$) by using an integer d_i and random number v_i.

22. The encryption method of claim 21, wherein

$\gcd(V_i, d_i) = 1$ is satisfied.

23. The encryption method of claim 21, wherein

the ciphertext is obtained based on a product-sum operation

of the components of said fourth vector and components of said fifth vector modulo-transformed based on said sixth vector.

24. The encryption method of claim 15, wherein

said fifth vector is generated using L sets ($L \geqq 2$)of sixth vector whose K components $D_i^{(y)}$ ($1 \leqq i \leqq K$, $1 \leqq y \leqq L$)are respectively set such that $D_i^{(y)} = d^{(y)}/d_i^{(y)}$ (where $d^{(y)} = d_1^{(y)}d_2^{(y)}...d_K^{(y)}$) in each set by using L sets of integers $d_i^{(y)}$.

25. The encryption method of claim 24, wherein

the ciphertext is obtained based on a product-sum operation of the components of said fourth vector and components of said fifth vector modulo-transformed based on said sixth vector.

26. The encryption method of claim 15, wherein

said fifth vector is generated using L sets ($L \geqq 2$)of sixth vector whose K components $V_i^{(y)}$ ($1 \leqq i \leqq k+n$, $1 \leqq y \leqq L$) are respectively set such that $V_i^{(y)} = (d^{(y)}/d_i^{(y)}) \cdot v_i^{(y)}$ (where $d^{(y)} = d_1^{(y)}d_2^{(y)}...d_K^{(y)}$) in each set by using L sets of integers $d_i^{(y)}$ and random numbers $v_i^{(y)}$.

27. The encryption method of claim 26, wherein

$\gcd(V_i^{(y)}, d_i^{(y)}) = 1$ is satisfied.

28. The encryption method of claim 26, wherein

$\gcd(d_i^{(y)}, d_j^{(y)}) = 1$ $(1 \leqq j \leqq K)$ is satisfied.

29. The encryption method of claim 26, wherein

the ciphertext is obtained based on a product-sum operation of the components of said fourth vector and components of said fifth vector modulo-transformed based on said sixth vector.

30. A decryption method for decrypting a ciphertext obtained using the encryption method of claim 1, wherein

the components of said plaintext vector are decrypted independently of the components of said random number vector.

31. A decryption method for decrypting a ciphertext obtained using the encryption method of claim 1, wherein

the ciphertext is decrypted into the plaintext while identifying positions of the components of said plaintext vector.

32. A decryption method for decrypting a ciphertext obtained using the encryption method of claim 15, wherein

the ciphertext is decrypted into the plaintext while identifying positions of the components of said first vector.

33. A cryptographic communication method for performing information communication between entities, comprising the steps of:

creating a ciphertext from a plaintext at a first entity, according to the encryption method of claim 1, and transmitting the ciphertext to a second entity; and

decrypting the transmitted ciphertext into the plaintext at the second entity,

wherein positions of the components of said plaintext vector or the components of said random number vector in said composite vector are set at the first entity, and information indicating the set positions is sent to the second entity.

34. The cryptographic communication method of claim 33, wherein

the information indicating the set positions is included in a ciphertext to be created, and the ciphertext including the information is transmitted to the second entity.

35. A cryptographic communication method for performing information communication between entities, comprising the steps of:

creating a ciphertext from a plaintext at a first entity, according to the encryption method of claim 1, and transmitting the ciphertext to a second entity; and

decrypting the transmitted ciphertext into the plaintext at the second entity,

wherein positions of the components of said plaintext vector

or the components of said random number vector in said composite vector are set at the second entity, and information indicating the set positions is sent to the first entity.

36. A cryptographic communication system for performing information communication using ciphertext between entities, comprising:

an encryptor for creating a ciphertext from a plaintext by using the encryption method of claim 1;

a communication channel for transmitting the created ciphertext from a first entity to a second entity; and

a decryptor for decrypting the transmitted ciphertext into the plaintext.

37. A computer memory product having computer readable program code means for causing a computer to create product-sum type ciphertext from plaintext, said computer readable program code means comprising:

program code means for causing the computer to create a composite vector by adding a random number vector whose components are a plurality of arbitrarily selected random numbers to a plaintext vector having a plurality of components obtained by dividing a plaintext to be encrypted; and

program code means for causing the computer to create a ciphertext by using said composite vector and a publicized public

vector.

38. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to create product-sum type ciphertext from plaintext, comprising:

a code segment for causing the computer to create a composite vector by adding a random number vector whose components are a plurality of arbitrarily selected random numbers to a plaintext vector having a plurality of components obtained by dividing a plaintext to be encrypted; and

a code segment for causing the computer to create a ciphertext by using said composite vector and a publicized public vector.